UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/758,114 | 01/16/2004 | Shinsuke Suzuki | HITA.0495 | 4985 |

7590 11/19/2008

Stanley P. Fisher
Reed Smith LLP
Suite 1400
3110 Fairview Park Drive
Falls Church, VA 22042-4503

| EXAMINER | |
|---|---|
| NAJEE-ULLAH, TARIQ S | |
| **ART UNIT** | **PAPER NUMBER** |
| 2456 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 11/19/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/758,114 | SUZUKI ET AL. | |
| | Examiner | Art Unit | |
| | TARIQ S. NAJEE-ULLAH | 2456 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *16 September 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-3,6-8,10,11 and 13-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,6-8,10,11 and 13-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Continued Examination Under 37 CFR 1.114*

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on September 16, 2008 has been entered.

### *Response to Amendment*

2. Claims1-3,6-8,10,11 and 13-19 are pending in the case. Claims 1-2, 6-8, 10-11, 14-15 and 17-19 have been amended. Claim 12 has been cancelled by amendment.

### *Response to Arguments*

3. Applicant's arguments filed September 16, 2008 have been fully considered but they are not persuasive. Applicant argues that "Neuman does not show or suggest determining whether there is a logical conflict among traffic control requests (see Remarks, pg. 9 of response)." Examiner respectfully disagrees. Neuman discloses the invention features "*full Firewalling; rules downloaded from server based on either the machine (MAC address) or the user ID… filtering based on connection identification information (match current firewall capabilities)…* (Neuman, pg. 3, par. 46)." Filtering based on connection information inherently implies use of a MAC address, IP address or user ID of the client sending the packet. Both the IP address and user ID are logical identifiers. Examiner interprets filtering based on connection information to be a

comparison of the source IP address or user ID from a packet sender with the IP address or user ID stored on the CMC. In Neuman's invention, IP addresses are mapped to a user ID which is managed by the CMC (Neuman, pg. 3, par. 50). This is even more explicitly taught by Neuman as Neuman further discloses "…*filtering based on both endpoints; capability to drop anonymous packets…*(Neuman, pg. 3, par. 46)." Inherently, a positive notification of no conflict of user IDs has clearly been performed if the connection is made. If the connection is refused, a notification of a conflict of user IDs has clearly been made and the proper action has been taken.

In conclusion, in an effort to better place the claims in condition for allowance, Examiner encourages the modification of claim language to include language that is more precisely descriptive and provides a more clear representation of what the Applicant presents as the invention in the specification in a manner which overcomes the prior art as presented. Examiner also reminds Applicant that although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

### ***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-3, 6-8, 10-11, and 13-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Publication Number 2002/0162026 to Neuman et al (Neuman hereinafter) in view of US Publication Number 2003/0035371 to Reed et al (Reed hereinafter).

Regarding claims 1, 10, 17, and 18, Neuman discloses **a traffic control computing device comprising: a traffic control interface connected to traffic control devices which control traffic in a network** (Neuman, Figure 1A, Page 1, paragraph [0002]; Neuman discloses each node or computer on the network has a secure, intelligent network interface, i.e. traffic control interface, with a coprocessor that handles all network communication, i.e. control traffic in a network.)**; a traffic control request interface connected to traffic control request detecting devices which determine whether a traffic control must be executed by said traffic control devices** (Neuman, Fig. 3; Pg. 5, Par. [0071]; Neuman discloses the present invention, as illustrated in FIG. 3, places a secure, intelligent network interface, i.e. traffic control request interface, between the user workstation and the Internet and server, i.e. traffic control request detecting device, so as to provide firewall, i.e. traffic control device, features across all layers of the protocol stack, including filtering, i.e. determining whether a traffic control must be executed, based upon Distinguished Name or the authenticated universally unique username.)**; a first storage device in which information about traffic control received via the traffic control request interface is stored** (Neuman, Pg. 3, par. [0047]; Neuman discloses user/passwords can be stored on the centralized management system and given out securely and on an as

needed basis to the clients. The word "stored" inherently refers to some type of storage device or medium that is part of the centralized management system. Users and passwords are information associated with traffic control.)**; a traffic control computing unit connected to said traffic control interface** (Neuman, Fig. 1A, Pg. 1, par. [002]; Neuman discloses each node or computer on the network has a secure, intelligent network interface, i.e. traffic control interface, with a coprocessor, i.e. traffic control computing unit, that handles all network communication)**, and connected to said traffic control request interface** (Neuman, Pg. 1, par. [0002]; Neuman discloses each node or computer on the network has a secure, intelligent network interface, i.e. traffic control request interface, with a coprocessor, i.e. traffic control computing unit, that handles all network communication)**, and connected to said first storage device** (Neuman, Pg. 3, par. [0047]; Neuman discloses user/passwords can be stored on the centralized management system and given out securely and on an as needed basis to the clients. The word "stored" inherently refers to some type of storage device or medium that is part of the centralized management system. Users and passwords are information associated with traffic control.)**; and a traffic control computing management interface** (Neuman, Figure 1A, central management console)**, wherein said traffic control computing unit computes traffic control algorithms based on traffic control requests received from said traffic control request detecting devices and stored in the first storage device and sends the traffic control algorithms to said traffic control interface** (Neuman, Pg. 1, par. [0002]; Neuman discloses the intelligent network interface encrypts outgoing packets and decrypts

incoming packets from the network based on a key and algorithm, i.e. traffic control algorithms, managed, i.e. computed, by a centralized management console (CMC), i.e. the main traffic control computing unit, on the network. Pg. 2, par. [0031]; For a client to initiate a connection with the server, the client's secure, intelligent network interface sends a request to the central management console (CMC) with the identifying information about the connection that the client wishes to send to the server.), **wherein said traffic control computing unit compares information about a sender of a second traffic control request received through said traffic control request interface for a match with any of traffic control information objects stored in said first storage device and rejects said second traffic control request if the information about said sender of the second request is not stored in said first storage device, wherein said traffic control computing management interface is configured to operate as a contact point for communicating with a network administrator and wherein said traffic control computing unit checks whether said second traffic control request received logically conflicts with any traffic control request stored in said first storage device** (Neuman, pg. 3, par. 46, 50) **and, if said second traffic control request received logically conflicts with any traffic control request stored in said first storage device** (Neuman, pg. 3, par. 46, 50)**, compares information about the sender of the second traffic control request with information about the sender of said traffic control request that logically conflicts with said second traffic request received** (Neuman, pg. 3, par. 46, 50)**, and, if both the senders are different, sends a notification of the logical confliction to said**

**traffic control computing management interface.** Neuman does not explicitly teach all elements of the claimed invention.

Reed discloses **wherein said traffic control computing unit** (Reed, pg. 5, par. 53; congestion-fee switching system) **compares a sender of a traffic control request** (Reed, pg. 5, par. 53, request controller) **received through said traffic control request interface** (Reed, pg. 5, par. 53, request controller) **for a match with any of traffic control information objects** (Reed, pg. 5, par. 53, priority information) **stored in said first storage device and rejects said traffic control request if said sender of the received request is not stored in said first storage device** (Reed, pg. 5, par. 56, request controller sends rejection responses)**; and wherein said traffic control computing management interface** (Reed, fig. 1D, 140) **is configured to operate as a contact point for communicating with a network administrator** (Reed, pg. 15, par. 186; system processor communicates with a global administration and management system)**; and said traffic control computing unit** (Reed, pg. 5, par. 53; congestion-fee switching system) **checks whether a traffic control request that conflicts with said traffic control request received is included in said first storage device and, if a conflicting traffic control request is included, compares a sender of the conflicting traffic control request with the sender of said traffic control request received, and, if both the senders are different, sends a notification of the conflicting requests to said traffic control computing management interface** (Reed, pg. 2, par. 15; Control information is sent to resolve data transmission conflicts in the interconnect structure where each node is a successor to a node on an adjacent

outer level and an immediate successor to a node on the same level. Message data from an immediate predecessor has priority. Control information is sent from nodes on a level to nodes on the adjacent outer level to warn of impending conflicts.).

Neuman and Reed are analogous art because they are from the same field of endeavor of network communication. At the time of the invention, it would have been obvious to a person of ordinary skill in the art to use Reed's traffic control methods with Neuman's invention. The suggestion/motivation would have been to provide for a more efficient, congestion-free switching system (Reed, pg. 4, par. 49).

Regarding claim 2, Neuman-Reed discloses the invention substantially as described in claim 1 above including, **an information unit for acquiring information objects about traffic control details per traffic control device associated with IDs of the traffic control devices, the traffic control details being now executed separately by said traffic control devices** (Pg. 1, par. [0002]; Neuman discloses each node or computer on the network has a secure, intelligent network interface, i.e. traffic control interface, with a coprocessor, i.e. an information unit, that handles all network communication. Pg. 3, par. [0046]; Neuman further discloses each node (client, server, mainframe, etc.) should feature rules downloaded from server based on either the machine (MAC address) or the user ID.)**; and a second storage device in which said acquired information objects about traffic control details per traffic control device associated with the IDs of the traffic control devices are stored** (Pg. 4, par. [0069]; Neuman discloses all authentication information is stored on a Central Management Console (CMC) implying CMC also functions as a second storage device. Pg. 5, par.

[0071]; Neuman discloses the present invention, places a secure, intelligent network interface between the user workstation and the Internet and server so as to provide firewall features across all layers of the protocol stack, including filtering based upon Distinguished Name or the authenticated universally unique username, i.e. associated IDs of the traffic control devices.).

Regarding claim 3, Neuman-Reed discloses the invention substantially as described in claim 1 above including, **wherein IDs of said traffic control request detecting devices are stored in said first storage device** (Neuman, Pg. 3, par. [0047]; Neuman discloses the invention allows transparent single sign on to any device, i.e. traffic control request detecting device, using applications or servlets supplied by the Central Management Counsel (CMC) to allow user/password, i.e. IDs, to be negotiated automatically. User/passwords can be stored on the centralized management system and given out securely and on an as needed basis to the clients. The word "stored" inherently refers to some type of storage device or medium that is part of the centralized management system.).

Regarding claim 6, Neuman-Reed discloses the invention substantially as described in claim 1 above including, **wherein, if both said senders match, said traffic control computing unit is structured to assume that said sender of said traffic control request that conflicts with the second traffic control request sent a request to cancel said traffic control request that conflicts with the second traffic control request** (Fig. 4, Pg. 6, par. [0089]; Neuman discloses in addition to making security functions universal, the invention makes them centrally manageable. A network

administrator can specify policies, update agents, patch vulnerabilities, track usage, and manage users all from a central management server. Pg. 6, par. [0093]; Neuman further discloses the invention maintains a cache of servlets that are regularly checked, i.e. compared, against the master repository on the CMC. These servlets translate the requests into manageable instructions.).

Regarding claim 7, Neuman-Reed discloses the invention substantially as described in claim 2 above including, **wherein, when said information acquiring unit has been successful in newly acquiring a traffic control information object from a traffic control device among the traffic control devices** (fig. 5Neuman teaches a secure network interface, i.e. traffic control device at each client)**, said traffic control computing unit is structured to determine that said traffic control device is operating and updates the traffic control information object for the traffic control device among the traffic control devices** (fig. 5Neuman teaches a secure network interface, i.e. traffic control device at each client) **stored in said first storage device to said traffic control information object newly acquired** (Pg. 3, par. [0043]; Neuman discloses memory can include updateable flash memory for the OS. An input is included for physical identification requirements, whether directly connected to the client machine, such as a serial, USB or parallel port, or implemented as a port, such as a USB port or parallel port, on the secure, intelligent network interface.).

Regarding claim 8, Neuman-Reed discloses the invention substantially as described in claim 2 above including, **wherein that when a traffic control information object has failed to be acquired from a traffic control device among**

**the traffic control devices** (fig. 5Neuman teaches a secure network interface, i.e. traffic control device at each client)**, said traffic control computing unit determines that said traffic control device among the traffic control devices** (fig. 5Neuman teaches a secure network interface, i.e. traffic control device at each client)**is not operating and deletes the traffic control information object for the traffic control device determined as being non-operating from said storage device** (Fig. 9, Pg. 5, par. [0076; Neuman discloses the present invention provides non-host integrated fault tolerance. Fault tolerance is implemented between machines without needing to install any software or hardware on the critical machines. As illustrated in FIG. 9, by monitoring the server, i.e. traffic control device, from its network connection to ensure that it is still up or not, the secure, intelligent network interface can identify when functionality needs to be moved to the backup server. Although illustrated with respect to servers, it can be implemented on any machine, be it a workstation, mainframe, etc., that includes the interface of the present invention.)**.**

Regarding claim 11, Neuman-Reed discloses the invention substantially as described in claim 10 above including, **if said conflict exists, determining whether said sender of the received request and the sender of the control request match** (Fig. 4, Pg. 6, par. [0093]; Neuman further discloses the invention maintains a cache of servlets that are regularly checked, i.e. compared, against the master repository on the CMC. These servlets translate the requests into manageable instructions. Pg. 3, par. [0047]; Neuman discloses user/passwords can be stored on the centralized management system and given out securely and on an as needed basis to the clients)

**that logically conflicts with the received traffic request** (Neuman, pg. 3, par. 46, 50)**; and if both the senders match, deleting said control request logically conflicts with the received traffic request** (Neuman, pg. 3, par. 46, 50) **from said storage device** (Pg. 6, par. [0095]; Neuman discloses if the login request, i.e. traffic control request, is not successful, i.e. deleted, the system prompts the client for the username and password, which it then sends to the CMC for storage, and repeats the procedure until the user is logged in, or gives up. It is inherent that the login request, i.e. traffic control request, is removed since no access is granted unless the proper login information is stored on the CMC. Since the login request fails to produce the users desired result, it is inherent that the request has been deleted by the CMC.)**.**

Regarding claim 13, Neuman-Reed discloses the invention substantially as described in claim 10 above including, **determining whether the sender of the received traffic control request is from a pre-registered sender device** (Neuman, Fig. 4, Pg. 6, par. [0093]; Neuman further discloses the invention maintains a cache of servlets that are regularly checked, i.e. compared, against the master repository on the CMC. Pg. 3, par. [0047]; Neuman discloses user/passwords can be stored, i.e. pre-registered, on the centralized management system and given out securely and on an as needed basis to the clients. The word "stored" inherently refers to some type of registration or saving on a storage device or medium that is part of the centralized management system.)**; and rejecting the control request from a non-registered sender** (Neuman,Pg. 6, par. [0095]; Neuman discloses if the login request, i.e. traffic control request, is not successful, i.e. rejected, the system prompts the client for the

username and password, which it then sends to the CMC for storage, and repeats the procedure until the user is logged in, or gives up. It is inherent that the login request, i.e. traffic control request, is rejected since no access is granted unless the proper login information is stored, i.e. pre-registered, on the CMC. Since the login request fails to produce the users desired result, it is inherent that the request has been rejected by the CMC.).

Regarding claim 14, Neuman-Reed discloses the invention substantially as described in claim 13 above including, **wherein, if said sender of the received traffic control request is a pre-registered sender, said step of determining whether said received traffic control request logically conflicts** (Neuman, pg. 3, par. 46, 50) **with any of control requests previously stored in said storage device is executed** (Pg. 6, par. [0095]; Neuman discloses if the login request, i.e. traffic control request, is not successful, i.e. rejected, the system prompts the client for the username and password, which it then sends to the CMC for storage, and repeats the procedure until the user is logged in, i.e. the request is executed, or gives up.).

Regarding claim 15, Neuman-Reed discloses the invention substantially as described in claim 10 above including, **receiving information as to whether said network administrator has rejected a part or all of either of the conflicting control requests** (Fig. 4, Pg. 6, par. [0089]; Neuman discloses in addition to making security functions universal, the invention makes them centrally manageable. A network administrator can specify policies, update agents, patch vulnerabilities, track usage, and manage users all from a central management server.) **that conflicts with the**

**traffic control request stored in the storage device** (Neuman, pg. 3, par. 46, 50)**; and notifying the sender of the rejected control request that the control request logically conflicts with the traffic control request stored in the storage device** (Neuman, pg. 3, par. 46, 50) **was rejected** (Pg. 6, par. [0095]; Neuman discloses if the login request, i.e. traffic control request, is not successful, i.e. rejected, the system prompts the client for the username and password, which it then sends to the CMC for storage, and repeats the procedure until the user is logged in, or gives up. It is inherent that the login request, i.e. traffic control request, is rejected since no access is granted unless the proper login information is stored, i.e. pre-registered, on the CMC. Since the login request fails to produce the users desired result, it is inherent that the request has been rejected by the CMC.)**.**

Regarding claim 16, Neuman-Reed discloses the invention substantially as described in claim 10 above including, **comparing said computed control algorithm with control algorithms separately held by the traffic control devices connected to the computing device** (Neuman, Pg. 1, par. [0002]; Neuman discloses the intelligent network interface encrypts outgoing packets and decrypts incoming packets from the network based on a key and algorithm, i.e. traffic control algorithms, managed, i.e. computed, by a centralized management console (CMC), i.e. the main traffic control computing unit, on the network.)**; if said computed control algorithm is not held by said traffic control devices, transmitting the computed control algorithm to the appropriate one of said traffic control devices** (Neuman,Pg. 1,

par. [0011]; Neuman discloses the secure, intelligent network interface can apply the appropriate encryption algorithm to the appropriate network device.).

Regarding claim 19, Neuman-Reed discloses the invention substantially as described in claim 18 above including, **acquiring second information which comprises identifiers of said traffic control devices and the traffic control functions of traffic control devices** (Pg. 3, par. [0047]; Neuman discloses user/passwords can be stored on the centralized management system and given out securely and on an as needed basis to the clients. The word "stored" inherently refers to some type of storage device or medium that is part of the centralized management system. Users and passwords are information associated with traffic control.)**; and storing said second information acquired into the storage device** (Pg. 4, par. [0069]; Neuman discloses all authentication information is stored on a Central Management Console (CMC) implying CMC also functions as a second storage device. Pg. 5, par. [0071]; Neuman discloses the present invention, places a secure, intelligent network interface between the user workstation and the Internet and server so as to provide firewall features across all layers of the protocol stack, including filtering based upon Distinguished Name or the authenticated universally unique username, i.e. associated IDs of the traffic control devices.)**, wherein, if the control algorithm calculated by said traffic control computing device has already been held by one of said traffic control devices, said traffic control computing device does not transmit the calculated control algorithm** (Pg. 1, par. [0002]; Neuman discloses the intelligent network interface encrypts outgoing packets and decrypts incoming packets

from the network based on a key and algorithm, i.e. traffic control algorithms, managed, i.e. computed, by a centralized management console (CMC), i.e. the main traffic control computing unit, on the network. Pg. 2, par. [0031]; For a client to initiate a connection with the server, the client's secure, intelligent network interface sends a request to the central management console (CMC) with the identifying information about the connection that the client wishes to send to the server.).

***Conclusion***

6. In conclusion, in an effort to better place the claims in condition for allowance, Examiner encourages the modification of claim language to include language that is more precisely descriptive and provides a more clear representation of what the Applicant presents as the invention in the specification in a manner which overcomes the prior art as presented. Examiner also reminds Applicant that although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TARIQ S. NAJEE-ULLAH whose telephone number is (571)270-5013. The examiner can normally be reached on Monday through Friday 8:30 - 6:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bunjob Jaroenchonwanit can be reached on (571) 272-3913. The fax

phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/TN/

/Philip C Lee/
Primary Examiner, Art Unit 2452